DYNAMIC ANTI-MONEY LAUNDERING SYSTEM AND METHODOLOGY FOR PROVIDING SITUATIONAL-SPECIFIC RISK ASSESSMENT DETERMINATIONS

5

FIELD OF THE INVENTION

10   [001]   The present invention relates to the field of enterprise risk management. More specifically, the present invention provides an improved Anti-Money Laundering (AML) system and methodology for a financial institution that provides dynamic, contextually-driven compliance action analyses, guidance and recommendations, which may be based on predetermined risk dimensions of the financial institution or a

15   particular branch of the financial institution, in order that situational-specific risk assessments may be made at the level of a particular site or branch of the financial institution.

BACKGROUND OF THE INVENTION

20

[002]   Money laundering is a global concern that poses a significant threat to the world's financial institutions. This threat has blossomed in recent years in view of the advent of increased global electronic financial transactions. In the United States, regulators have taken an explicit approach to specifying the requirements of AML

25   programs. Recent regulatory changes in the United States brought about by the USA Patriot Act of 2001, Public Law 157-56 to the "Currency and Foreign Transactions Reporting Act" (also known as the "Bank Secrecy Act" (BSA)), 31 U.S.C. §§ 1051 et seq., and ensuing regulations have significantly increased both the number of financial institutions that must implement Anti Money Laundering (AML) policies

30   and the complexity of the requirements. The regulations require, *inter alia*, reporting of large cash transactions, retention of records, and the reporting of suspicious transactions and behaviors to the Financial Crimes Enforcement Network (FinCEN). Other regulators have taken less direct approaches, requiring banks to implement effective, risk-based programs, while leaving implementation details to the discretion

35   of the institution. While it would seem that such a less-direct approach might be easier to implement, it is not necessarily so, since the institution is still required to implement solutions that are consistent with its level of exposure and risk, and the

institution will have less guidance as to how to effectively realize such solution. In all cases, Failure to implement such policies in a satisfactory manner exposes the institute, as well as individual Compliance Officers to significant fines. Institutions also face risk to their respective reputations and goodwill should they be found lax in

5   preventing money laundering and terrorism.

[003]   A globally important element of the regulations is that these AML policies require a "risk-based" approach to selecting appropriate measures. That is, organizations are required to identify and evaluate correctly the risk exposures

10   associated with each area of operation and then apply counter measures that appropriately match the risk. The rational used to choose these counter measures must be consistent, explainable, and defendable.

[004]   Anti Money Laundering (AML) solutions are an enterprise-wide undertaking

15   involving multiple constituencies both within the organization and outside it. Internally, the initiative requires the coordinated effort of a large number of employees across multiple geographical locations. Externally, the effort is likely to involve ongoing communication with law-enforcement agencies as well as satisfying and giving comfort to regulatory agencies.

20

[005]   Training employees to perform their respective roles effectively in this area can be a significant challenge, considering that most financial institution employees have little or no background in law enforcement. Obtaining the approval of the various regulatory agencies also depends on the ability to articulate and communicate

25   the rationale behind the AML program. For example, what risks have been identified? How was the severity of each of these risks at different geographical locations evaluated? Why is it believed that the measures taken are effective in addressing those risks?

30   [006]   The current generation of AML solutions focuses merely on the detection of transactions that look suspicious. These solutions usually employ various algorithms to try to identify which transactions should be flagged for further review. The problem with these AML solutions is that while they may adequately detect certain suspicious transactions, they do not take into account a significant number of

important factors that can affect an appropriate evaluation of the risk exposures as associated with a particular area of operation, nor do the solutions assist in determining the appropriate counter measures that should be applied once it has been determined that there is a risk exposure. For example, some areas in which current

5   AML solutions are lacking include:

1). Effective guidance once a suspicion is flagged. Current AML systems do not give assistance regarding what should be done with flagged suspicions. Since current systems generate a high volume of "false positives", and there are risks in being either too lenient or too strict, institutions need a way to deliver advice to the

10   point where it is needed.

2). Enterprise-based consistency. Because institutes are required by law to develop "risk based" policies, they need a means for implementing a consistent approach across the organization and for communicating their rational to regulators.

3). Access prevention. AML regulations cover more than just the monitoring

15   of transactions. Due diligence procedures during account opening is another area where expertise is required. Again institutions must balance between the risk of failing to turn away criminals and the lost business involved in turning away a profitable customer.

4). Experience. Most employees of a financial organization have no

20   experience in law enforcement. Training, monitoring, and coordinating problem escalation channels across the organization pose a major "change management" issue that is currently only partially addressed.

[007] Accordingly, an improved AML methodology is needed that will take into

25   account factors that can affect an appropriate evaluation of the risk exposures associated with a particular area of operation or transaction, and that can assist a financial institution's Compliance Officer or other authorized user in determining the appropriate counter measures that should be applied for a particular site or branch once it has been determined that there is a risk exposure.

30

SUMMARY OF THE INVENTION

[008] The present invention provides an improved Anti-Money Laundering (AML) system and methodology for a financial institution that provides dynamic,

contextually-driven compliance action analyses, guidance and recommendations. The compliance action analyses, guidance and recommendations provided by the AML system and methodology of the present invention may be based on predetermined risk dimensions of the financial institution or a particular branch of the financial

5   institution, and may be overridden by a Compliance Officer or other authorized user based on alternate analyses, guidance and recommendations provided by the AML system and methodology in view of the context or facts of the particular operation or transaction at the particular location.

10   [009]   According to one aspect of an embodiment of the present invention, risk dimensions are assigned to describe the risk profile of a particular site or branch of a financial institution. Additionally, handling procedure levels or categories are determined for each particular site or branch of a financial institution. Depending upon the nature and characteristics of the particular operation or transaction

15   conducted by the financial institution, and the risk profile of a particular site or branch of a financial institution the category or level of the handling procedure that should be used for that particular operation or transaction at the particular institution or branch is based on one or more of the determined risk dimensions.

20   [010]   According to another aspect of an embodiment of the present invention, risk dimensions for a financial institution or branch of a financial institution are identified and assigned numerical designations. The type of financial transaction to be conducted at the branch of a financial institution is then identified and it is further determined whether the financial transaction has a risk-related dimension and, if so,

25   whether the numerical designation of at least a selected one of the identified risk dimensions exceeds a predetermined level. If the numerical designations of at least a selected one of the identified risk dimensions exceeds a predetermined level, a special risk assessment procedure is performed and recommended guidelines for handling the financial transaction based on the special risk assessment procedure are provided to an

30   authorized user.

[011]   According to yet another aspect of an embodiment of the present invention, there are at least four risk dimensions. A first risk dimension represents the risks due to the location of the branch of the financial institution and a second risk dimension

represents the risks due to selected services offered by the branch of the financial

institution. A third risk dimension represents the risks due to the nature of the

customers served by the branch of the financial institution, and a fourth risk

dimension represents the risks due to the jurisdictions served by the financial

5   institution.

[012] According to still another aspect of an embodiment of the present invention, the

Anti-Money Laundering system includes a risk assessor module for providing to an

authorized user of the anti-money-laundering system, guidelines in identifying risks

10   associated with the branch of the financial institution, and a policy builder module for

recommending possible electronic and manual countermeasures to the risks identified

by the risk assessor module and for enabling the authorized user to select the

countermeasures of his choice in order to create a policy for the branch of the

financial institution. The system further includes an account opening due diligence

15   module for providing detailed recommendations to the authorized user as to whether

to allow an application for account at the branch of the financial institution and for

applying consistent implementation of the policy throughout the branch of the

financial institution, and a transaction activity monitor module for receiving and

monitoring transaction information including transaction information received by the

20   account opening due diligence module, and for identifying suspicious patterns among

the transactions at the branch of the financial institution in order to provide a

suspicious transaction activity report. A case management and reporting module

tracks and identifies the detailed recommendations of the account opening due

diligence module in order to provide continuous feedback to the authorized user about

25   the effectiveness of the system

[013] According to still another aspect of an embodiment of the present invention, the

risk dimensions that are used in forming the compliance action analyses, guidance and

recommendations are based on local laws, regulations, historical data, and other

30   information that are specific to a particular site or branch of the financial institution.

[014]   According to another aspect of the present invention, the Anti-Money

Laundering (AML) system and methodology of the present invention provides

alternative compliance action analyses, guidance and recommendations which the

Compliance Officer or other authorized user may use to override the initial
compliance action analyses, guidance and recommendations, based on the on the
context or facts of the particular operation or transaction presented to the Compliance
Officer or other authorized user.

5

[0015] Other features of the present invention will become evident hereinafter.

BRIEF DESCRIPTION OF THE FIGURES

10   [016]   The foregoing summary, as well as the following detailed description, is better
understood when read in conjunction with the appended drawings. For the purpose of
illustrating the invention, there is shown in the drawings exemplary constructions of
the invention; however, the invention is not limited to the specific methods and
instrumentalities disclosed. In the drawings:

15

[017]   FIG. 1 shows a diagram of one embodiment of the dynamic AML system of
the present invention.

[018]   FIG. 2 shows a preferred embodiment of the AML logic of the dynamic AML
20   system of the present invention.

[019]   FIG. 3 is a flowchart showing the processing and identification of situational-
specific risks by the Risk Assessor Module;

25   [020]   FIG. 4 is flowchart showing an embodiment of risk dimension determination
in accordance with a preferred embodiment of the dynamic AML system of the
present invention.

DETAILED DESCRIPTION OF THE INVENTION
30

[021]   Referring to FIG. 1, the present invention provides an improved Anti-Money
Laundering (AML) system 10 for a financial institution that provides dynamic,
contextually-driven compliance action analyses, guidance and recommendations
preferably based on predetermined risk dimensions of the financial institution or a

particular branch of the financial institution. In a preferred embodiment of the AML system 10 of the present invention, a detection engine 20 receives risk-related information via accessing a network of information 30, including federal, state and local criminal systems 40, federal, state and local repositories 50, and other

5   information, such as from human resources 60 (e.g., other branches of the same financial institution). The detection engine 20 communicates with the knowledge engine 70 of the AML system 10, the knowledge engine storing and applying previously garnered local laws, regulations, historical data, trade organization guidelines, expert analyses, and other information that is specific to a particular site or

10   branch of the financial institution. The AML system 10 provides compliance action analyses, guidance and recommendations to the Compliance Officer or other authorized user(s) 80. Preferably, the AML system 10 of the present invention also preferably provides alternative compliance action analyses, guidance and recommendations which the Compliance Officer or other authorized user may use to

15   override the initial compliance action analyses, guidance and recommendations, extend any grace period, or deny the customer application, in view of the context or facts of the particular operation or transaction at the particular location.

I. AML System Logic

20   [022] The AML system 10 may be embodied as any rule-based, Bayesian network, dynamic knowledge network, or other form of inference engines, and preferably, the AML system 10 of the present invention is communicatively coupled to an electronic network including a plurality of databases and other information sources, and collects and collates information from numerous various databases including, (i) government

25   sources; (ii) international organizations; (iii) regulatory agencies; (iv) self regulating trade organizations; and (v) commercial database firms. In one embodiment, the AML system and methodology of the present invention runs on Jnana Logic System 3.0, which is commercially available from Jnana Technologies Corporation, 469 Seventh Avenue, 13th Floor, New York, NY 10018. However, it will be appreciated

30   that the present invention is not so limited and may execute on any similar platform.

[023] In a preferred embodiment of the present invention, the AML system 10 includes the following modules:

A. Risk Assessor Module 90

[024]   The Risk Assessor Module 90 guides the Compliance Officer or other authorized user in identifying the unique risks associated with each branch or business unit of the financial institution including, among others, geographic location, types of customers served, types of services offered, jurisdictions served by the financial institution. The operation of this module will be discussion in more detail later with reference to FIG. 3.

B. Policy Builder Module 100

[025]   The Policy Builder Module 100 recommends possible electronic and manual counter measures to the risks identified and enables the Compliance Officer or other authorized user to select the measures of their choice. The system then creates a policy to fit the items selected. This module also functions in reverse order – describing the decision process that was involved in setting the policy. In this mode, the system is useful for defending the risk-based rationale behind the policy and any differences in policy between different business units.

C. Staff Training & Policy Management Module 110

[026]   The Staff Training and Policy Management Module 110 is an optional module extends the organization's selection of measures to developing customized training programs and to tracking student compliance. Students answer a questionnaire regarding the branch in which they work, as well as their areas of responsibility or job description. From that information, the system can construct a recommended training program, deliver the material, and track progress.

D. Account Opening Due Diligence Module 120

[027]   United States regulations are very specific about the due diligence required when opening new accounts. Other regulators are less specific, but nevertheless require prudent measures to eliminate potentially criminal persons. The Account Opening Due Diligence Module 120 ensures consistent implementation of due diligence procedures throughout the organization. As with other modules, use of expert-system technology allows rich explanations regarding why certain applications have been denied or which crucial pieces of information have still not been provided.

The system allows the authorized user to override any recommendations, to extend any grace period, or to deny the application.

E.   Transaction Activity Monitor Module 130

5   [028]   The Transaction Activity Monitor Module 130 monitors transaction and operation activities for suspicious patterns. Unlike other similar modules, which flag suspicious transactions but leave the bulk of the interpretation work to the Compliance Officer, or other authorized user, the Activity Monitor uses all available information – whether provided through activity scanning, during account opening

10   due diligence, or through random comments by bank personnel - to assemble the most likely scenario and to explain the suspicion in real world terms. Rather then merely reporting that the account's activity has increased by 10% over last month's, the Transaction Activity Monitor identifies and reports, via a suspicious transaction activity report, behaviors in meaningful "real-world" terms such as:

15

> *"Customer seems to avoid personal contact "*
> *"Customer attempts to mask large cash transactions", and/or*
> *"Customer's actions do not follow rational business sense"*

20   The information used may include historical and other data that is detected, collected, and consolidated with known methods and/or sensing devices, e.g., pattern recognition, rule-based filters, or other forms of fact-gathering, sensing, or knowledge discovery techniques.

F.   Case Management and Reporting Module 140

25   [029]   It is important in any AML system that when issues are raised, they subsequently be dealt with and resolved in a timely manner. The Case Management and Reporting Module 140 of the AML system 10 of the present invention accomplishes this function by ensuring that items are not dropped until they are either

30   resolved or dismissed. It also allows the authorized user to grant extensions and grace periods for gathering missing information or to cut short any further waiting. The case manager is also useful in providing continuous feedback regarding the effectiveness of the expert logic. By tracking and identifying those recommendations that are most often overridden, the Case Management and Reporting Module 140 can

35   assist the authorized user in improving system logic to minimize false alerts.

Similarly, the analysis can also detect employees that deviate from company policy by inappropriately overriding company procedures.

II. AML System Operation

5   [030]   In operation, and with reference to FIG. 3, the Risk Assessor Module 90 of the AML system 10 of the present invention first identifies the risk dimensions according to the type of operation/transaction that are carried out in the branch of the financial institution (Step 300). The Risk Assessor Module 90 then assigns numerical designations to thus identified risk dimensions (Step 305). Further detail regarding
10   risk dimensions will be had with reference to FIG. 4 in the subsequent paragraphs.

[031] After the Risk Assessor Module 90 assigns numerical designations to the identified risk dimensions, the type of financial transaction/operation to be conducted is identified (Step 310). The Risk Assessor Module 90 then determines whether the
15   financial transaction to be conducted has a risk-related dimension (Step 315). If the financial transaction/operation to be conducted does have a risk-related dimension, then the Risk Assessor Module 90 determines whether the numerical designation of at least a selected one of the risk dimensions identified in Step 300 exceeds a predetermined level (Step 320). If at least a selected one of the identified risk
20   dimensions exceeds a predetermined level, the Risk Assessor Module 90 performs a special risk assessment procedure (Step 325) and provides the output this procedure to the Policy Builder Module 100 (not shown), which provides compliance action analysis, guidance and recommendations to the Compliance Officer or other authorized user as to the handling of the particular financial transaction to be
25   conducted (Step 330).

[032] If none of the identified risk dimensions exceeds a predetermined level, the Risk Assessor Module 90 performs a standard risk assessment procedure (Step 335) and provides the output this procedure to the Policy Builder Module 100 (not shown). The
30   Policy Builder Module 100 will again provide compliance action analysis, guidance and recommendations to the Compliance Officer or other authorized user (Step 300); however, such analysis, guidance and recommendations will be based on a standard risk assessment, and thus likely different than those performed for a special risk assessment.

[033] Similarly, if at Step 315 it is determined that the financial transaction to be conducted does not have any risk-related dimensions, the determination of whether to perform a standard or special risk assessment will be determined on some other basis;

5 e.g., the average of risk dimensions for that particular transaction/operation (Step 340).

III. Risk Dimensions/Procedural Levels

[034] As discussed above, the AML system 10 of the present invention includes a

10 Risk Assessor Module 90 for guiding the Compliance Officer or other authorized user in identifying the unique risks associated with each branch or business unit of the financial institution. In one embodiment of the present invention, and with reference to FIG. 4, the risk dimensions determined by the Risk Assessor Module 90 include:

1). Risks due to location of the financial institution or branch of the financial

15   institution (Step 400);

2). Risks due to the type of services the financial institution offers or branch of the financial institution (Step 410);

3). Risks due to the nature of the customers served by the financial institution or branch of the financial institution (Step 420); and,

20   4). Risks due to the jurisdictions served by the financial institution (Step 430)

[035] The first and fourth risk dimensions may be arrived at by assigning a risk level to the various jurisdictions in which the branch or financial institution is or could be located. Both dimensions could be based on historical data regarding incidences

25 occurring in the location and jurisdiction in general, or on incidences particular to the financial institution or branch of the financial institution itself. The other two risk dimensions may come from data collected regarding the various selected services offered by the branch or financial institution, as well as the profile of the customers appearing in the institution's client base.

30

[036] The risk dimensions may be assigned a numerical designation (e.g., 1-10) or any other such scale. For example, at a financial institution or branch of the financial institution located in Cairo, Egypt, the following risks might be assigned:

Location risk -   3

Customer base risk -   4
Services offered risk -   2
Jurisdictions served risk - 3

5   [037] For each of the above risk dimensions, the number of accounts associated with a
given service type or belonging to a certain business type may also be tracked. The
risk in each category is determined by a count of items that have both high risk and
high exposure ratings (number of accounts).

10   [038] As set forth above, in operation, performance of a special or standard
assessment procedure is determined based on whether the financial transaction to be
conducted has a risk-related dimension, and whether the numerical designation of at
least a selected one of the risk dimensions exceeds a predetermined level. Referring
again to FIG. 3, if at least a selected one of the identified risk dimensions exceeds a
15   predetermined level, the Risk Assessor Module 90 performs a special risk assessment
procedure (Step 325).

[039] Thus, for example, a procedure for opening an account could be based on the
financial institution's or branch's risk dimensions in the "customer base" area, and
20   could be designated "special" if the branch is deemed to be serving a high-risk
clientele, or "standard," if the customer base is deemed to be of average risk. A
procedure for testing the financial institution's or branch's AML performance, on the
other hand, may be unrelated to any specific risk dimension, and the decision whether
to select a "standard" or "special" could be determined based on some other scale,
25   such as the average score in all four risk dimension categories. The objective is to
thus to establish logic that determines which level of each procedure should be used at
the institution or branch, based on one or more of the risk dimensions defined above.

[040] An operation or transaction that is designated "standard" may require an annual
30   review, while that designated "special" may require a semi-annual review or similar
designations, depending on the level of review that is deemed to be required. It will
be understood to those skilled in the art, that these are merely exemplary, and that
other distinctions may be made between a "standard" procedure and "special"
procedure.

IV. Procedure Override

[041] Referring again to FIG. 3, the AML system 10 preferably allows the Compliance Officer or other authorized user to override compliance action analysis, guidance and recommendations provided by the Policy Builder Module 100 (Step 345). Such might be the case, if the Compliance Officer or other authorized user deems that the context or facts of the particular operation or transaction at the particular location warrant different action that that recommended by the Policy Builder Module 100. In such a case, the Compliance Officer or other authorized user will provide alternate analyses, guidance and recommendations (Step 350). In the case where the transaction involves the opening of an account, the Case Management and Reporting Module 140 then tracks and identifies those recommendations that are most often overridden and updates the Account Opening Due Diligence Module based on the override.

[042] Thus, the improved AML system 10 of the present invention provides for the development of risk-based procedures that are site-or location-specific, and further allows for assistance in the articulation as to how these procedures were selected. The AML system 10 will provide for the (i) development, explanation, and defense of risk-based policies and procedures; (ii) development, explanation, and defense of risk-based training programs; (iii) determination of which new clients/customers to accept and which to reject; (iv) determination of which existing clients should be maintained and which should be rejected; and/or (vi) monitoring of ongoing business transactions for money laundering and/or other criminal and/or regulatory infractions. The improved AML system 10 of the present invention will also explain why certain transactions have been flagged as suspicious, provide the context behind selected transactions and simplifying further analysis of decision making, rank and prioritize flagged events and explain why some exceptions are considered more suspicious than others, explain the underlying rationale behind thresholds and limits, identify trends and typologies, and, leverage computer scanning and human interpretation to improve analysis.

[043] While the invention has been particularly shown and described with reference to various embodiments thereof, it will be understood by those skilled in the art that

13

various changes in form and details may be made therein without departing from the spirit and scope of the invention. Additionally, the present invention is by no means limited to use in the operating system environments discussed above, but rather, can be implemented in connection with any operating system.

5